

REMARKS

By this amendment, claims 1-29 are pending, in which claim 28 is currently amended. No new matter is introduced.

The Office Action (page 2) has imposed a 37 CFR § 1.105 Requirements for Information. In satisfaction of this rule, Applicants submit herewith an Information Disclosure Statement under 37 CFR § 1.97. With respect to the § 1.105 requirement, the Office Action, on page 2, states: "In response to this requirement, please provide the title, citation and copy of each publication that any of the applicants **relied upon to draft the claimed subject matter....**" Albeit the statement is a form paragraph (§ 7.117), Applicants do not understand the exact nature of the requirement, as § 1.105 (a)(1)(iv) pertaining to "Information used to draft application," merely stipulates the following: "A copy of any non-patent literature, published application, or patent (U.S. or foreign) that was **used to draft the application.**" (*Emphasis Added*) § 1.105 does not in fact make any requirement for information that was relied upon to draft "the claimed subject matter," but to draft "the application." Nevertheless, Applicants have made every effort to comply with the information requirement pursuant to § 1.105. Applicants submit herewith the following three documents: (1) Using the Border Gateway Protocol for Interdomain Routing, <http://www.cisco.com>, accessed 11/05/99; (2) Robert Stone, Center Track: An IP Overlay Network for Tracking DoS Floods, 10/01/99 (internal UUNET Technologies, Inc. document); and (3) Robert Stone, Center Track: An IP Overlay Network for Tracking DoS Floods, 10/01/99, Presentation, UUNET Technologies, Inc. Document (1) was relied upon for background information. The presentation, Document (3), was developed in light of the internal document (2); both of these documents were relied upon for various portions of the Specification.

The Office Action mailed September 30, 2003 rejected claims 1-8, 10-20, 22-24, and 26-29 as obvious under 35 U.S.C. § 103 based on *Gleichauf et al.* (US 6,301,668) in view of

Kovarik (US 6,014,628), and claims 9, 21, and 25 as obvious under 35 U.S.C. § 103 based on *Gleichauf et al.* in view of *Kovarik* and in further view of *Amicangioli et al.* (US 6,327,242).

Independent claim 1 recites “rerouting a DoS flood attack datagram to a tracking router, wherein the tracking router forms an overlay tracking network with respect to an egress edge router.” Independent claim 14 recites “a tracking router adjacent to the egress edge router, the tracking router being configured to perform the security diagnostic functions, the ingress edge router rerouting the DoS flood attack datagram to the tracking router as to permit identification of the ingress edge router, wherein the tracking router forms an overlay tracking network with respect to the plurality of edge routers.” Further, in the interest of expediting prosecuting, independent claim 28 has been amended to recite “receiving a DoS flood attack datagram on an overlay network formed by a tracking router.”

The Office Action, on page 4, asserts that *Gleichauf et al.* discloses the claimed tracking router forming an overlay network, citing FIG. 2 (block 20, 28), FIGs. 3 and 4 (block 110), col. 2: 58-60, col. 3: 7-13, col. 4: 57-67, col. 5: 1-32, and col. 6, 14-24. The Office Action presumes that *Gleichauf et al.*’s use of a network map (to which the several cited passages disclose) can reasonably lead to the conclusion that “the network security system discussed in *Gliechauf* could be replaced by a tracking router in order to provide a similar function as sought by the present claim limitations, namely that of forming a tracking network to discover where the attack is directed.” By this analysis, the Office Action appears to be acknowledging that *Gleichauf et al.* fails to disclose use of a “tracking router,” much less “wherein the tracking router forms an overlay tracking network.”

The legal basis for which the Office Action relies for its conclusion of obviousness, at best as can be understood, is a contorted notion of equivalence. MPEP § 2144.06 clearly states in order to rely on equivalence as a rationale supporting an obviousness rejection, the

equivalency must be recognized in the prior art, and cannot be based on applicant's disclosure or the mere fact that the components at issue are functional or mechanical equivalents. *In re Ruff*, 256 F.2d 590, 118 USPQ 340 (CCPA 1958). The use of a "tracking router" is not a recognized equivalent to a network security system that utilizes a network map; the basis for this strained interpretation stems not from the art, but from Applicants' disclosure.

Therefore, Applicants respectfully contend that a *prima facie* of obviousness has not been established. To establish *prima facie* obviousness of a claimed invention, all of the claim limitations must be taught or suggested by the prior art. *In re Royka*, 490 F.2d 981, 180 USPQ 580 (CCPA 1974). All words in a claim must be considered in judging the patentability of that claim against the prior art. *In re Wilson*, 424 F.2d 1382, 1385, 165 USPQ 494, 496 (CCPA 1970). The claims recite "wherein the **tracking router** forms an **overlay tracking network**."

To the extent that the Examiner is taking Official Notice of the claim features, pursuant to the MPEP § 2144.03, Applicants respectfully traverse the Official Notice and request the Examiner to produce references showing the claim features or withdraw the rejection as factually inadequate.

Furthermore, Applicants note that the conclusion of replaceability of *Gleichauf et al.* network security system 20 with the claimed tracking router has no technical merit. In fact, the notion of use of an overlay network is contrary to the operation of the *Gleichauf et al.* system.

Gleichauf et al. discloses (col. 5: 43 – col. 6: 65) that in operation, network security system 20 is operable detect attacks upon internal network 10. Network security system 20 accomplishes this by monitoring traffic on network backbone 14 and performing analysis tasks upon the monitored traffic in the context of network information discovered from internal network 10. In the embodiment of FIG. 1, scan engine 22 gathers the network information, while protocol engine 24 and signature engine 26 perform the analysis tasks upon the monitored traffic.

Scan engine 22 can direct requests upon the network and assess responses to such requests to discover network information. In one embodiment, scan engine 22 scans devices on internal network, such as workstations 12. For example, scan engine 22 could ping devices on internal network 10 and then perform port scans on each device. Banners from the port scans could be collected and analyzed to discover network information. Such network information could comprise the devices coupled to internal network 10, the operating systems running on such devices, and the services available on each device. Additionally, in the embodiment of FIG. 1, scan engine 22 is operable to analyze the network information to identify potential vulnerabilities of internal network 10, and confirm these potential vulnerabilities. Scan engine 22 can further create a network map 28 which can include such network information discovered by scan engine 22. Network map can comprise, for example, a multi-dimensional database with a real-time data insertion, as described in U.S. patent application Ser. No. 09/107,790, entitled "System and Method for Real-Time Insertion of Data Into a Multi-Dimensional Database for Network Intrusion Detection and Vulnerability Assessment," filed Jun. 30, 1998, pending, the disclosure of which is incorporated herein by reference.

As made clear from the above passage, the network security system 20 of *Gleichenhauf et al.* operates by monitoring traffic on network backbone 14 and performing analysis tasks upon the monitored traffic, as well creation of a network map. The backbone 14 is the actual network, not an overlay network; thus, monitoring of traffic of an overlay network and creating a map thereof would render the *Gleichenhauf et al.* system unfit for its intended purpose. In apparent recognition of this teaching away from the claimed invention, the Office Action conveniently embellishes the language of "overlay network" in its statement, "the network security system discussed in *Gleichenhauf* could be replaced by a tracking router in order to provide a similar function as sought by the present claim limitations, namely that of forming a tracking network to discover where the

attack is directed.” The claims do not recite a “tracking network.” Also, the Office Action’s replaceability argument is consistent with the teaching away, in that if indeed the functions of the *Gleichauf et al.* system and claimed invention are replaceable, then the redundant function would not be needed in the *Gleichauf et al.* system.

The secondary references of *Kovarik*, which is applied for a supposed teaching of an ingress edge router, and *Amicangoli et al.* (applied for its supposed teaching of communicating via physical connections) fail to disclose “wherein the tracking router forms an overlay tracking network.” The use of the language “tracking router” by *Kovarik* is only similar in words, the context is entirely different from the claimed features, as the tracking system of *Kovarik* tracks individuals and objects (see e.g., col. 1: 24-33; col. 1: 65 – col. 2:12), not DoS attacks. This distinction is further made evident in that *Kovarik* does not disclose or otherwise suggest any concept of an “overlay network.”

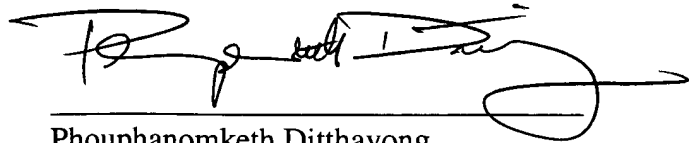
Accordingly, Applicants respectfully request the withdrawal of the obviousness rejections.

Therefore, the present application, as amended, overcomes the rejections of record and is in condition for allowance. Favorable consideration is respectfully requested. If any unresolved issues remain, it is respectfully requested that the Examiner telephone the undersigned attorney at (703) 425-8508 so that such issues may be resolved as expeditiously as possible.

Respectfully Submitted,

DITTHAVONG & CARLSON, P.C.

12/30/03
Date



Phouphanomketh Ditthavong
Attorney/Agent for Applicant(s)
Reg. No. 44658

10507 Braddock Road
Suite A
Fairfax, VA 22032
Tel. (703) 425-8508
Fax. (703) 425-8518